BY ORDER OF THE
SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 33-230

28 SEPTEMBER 2000

Communications and Information

INFORMATION PROTECTION ASSESSMENT AND ASSISTANCE PROGRAM

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the AFDPO WWW site at: http://afpubs.hq.af.mil.

OPR: HQ AFCA/GCIS (MSgt Donna Heaslip)
Certified by: HQ USAF/SCXX (Lt Col Pricer)
Supersedes AFI 33-230, 18 June 1999.
Pages: 14
Distribution: F

This instruction establishes the Information Protection Assessment and Assistance Program (IPAP). It applies to the Air Force Information Warfare Center (AFIWC), major commands (MAJCOM), field operating agencies (FOA), direct reporting units (DRU), information warfare squadrons (IWS), Headquarters Air Force Communications Agency (HQ AFCA), and all Air Force information systems users. Send recommended changes or comments to HQ AFCA/XPXP, 203 W. Losey Street, Room 1060, Scott AFB IL 62225-5222 using AF Form 847, **Recommendation for Change of Publication**, with an information copy to HQ AFCIC/SYIP, 1250 Air Force Pentagon, Washington DC 20330-1250. See **Attachment 1** for a glossary of references and supporting information.

SUMMARY OF REVISIONS

This IC changes the prescribed form from AFCOMSEC Form 13 to AF Form 4160 where referenced. Additionally, this IC corrects some minor administrative items. See the last attachment (**Attachment 4**) of the publication, IC 2000-1, for the complete IC. A (|) indicates revision from the previous edition.

1. General . The IPAPs purpose is to "find and fix" wing-level information protection (IP) problems. The IPAP accomplishes this by:

1.1. Assessing wing IP programs, the security posture of wing information systems, and the information contained within the systems.

1.2. Identifying and recommending solutions.

1.3. Helping to resolve problems.

1.4. Providing technical and training assistance including instructions in system accreditation and system policy development, when possible.

2. Responsibilities .

2.1. MAJCOMs:

2.1.1. Implement and manage a command IPAP. Send IPAP schedules to HQ AFCA/GCIS for tracking and monitoring.

2.1.2. Set up IP assessment and assistance (IPAA) teams (IPAT) consisting of personnel with experience in base information infrastructures, information systems, and IP Air Force specialty codes (AFSC).

2.1.3. Conduct biennial assessments of wing IP programs using AF Form 4160, **Information Assurance Assessment and Assistance Program (IAAP) Criteria**. If IPATs require technical support from the AFIWC, they must request it at least 60 days prior to scheduled MAJCOM IPAA visits. Gaining MAJCOMs will work with ANG to ensure biennial assessments of ANG units are performed.

2.1.4. Assessments. IPATs will assess:

2.1.4.1. Effectiveness of the wing IP program including IP operations function of the Air Force Network Control Center (AFNCC).

2.1.4.2. Security posture of wing information systems and the information contained therein.

2.1.4.3. Security of computer systems associated with information dependent systems such as, but not limited to, air traffic, base security alarm, sensor, and space systems.

2.1.4.4. Security, availability, and reliability of systems supporting the base information infrastructure.

2.1.4.5. Quality of wing communications security (COMSEC) operations (AFI 33-201, *[FOUO] Communications Security [COMSEC]*).

2.1.4.6. Quality of security training provided to individuals responsible for the operation of information systems, systems administrators, personnel responsible for COMSEC material, personnel assigned to the AFNCC, and wing IP personnel.

2.1.4.7. Actions taken based on Air Force computer emergency response team (AFCERT), automated systems security incident support team (ASSIST), and MAJCOM advisories.

2.1.4.8. Use of MAJCOM-developed annual summaries and analysis of IPAA reports.

2.1.5. Assistance. IPATs will:

2.1.5.1. Assist systems users, systems administrators, network managers, unit security personnel, AFNCC, and wing IP personnel in the resolution of identified problems to include, but not limited to, technical, administrative, and training. When IPATs cannot provide help, they will refer assessed organizations to the appropriate organizations for follow-on assistance.

2.1.5.2. Brief the senior host operational commander (normally the wing commander or designated representative) supported by the wing IP office, appropriate unit commanders, the commander exercising authority over the IP office, and the IP manager, on the posture of the wing IP program and the security of the base information infrastructure.

2.1.5.3. Develop an annual summary and analysis of IPAA reports and provide them to HQ AFCA, the AFIWC, and the command's wing IP office.

2.2. Wings:

2.2.1. Perform semiannual self-assessment of wing COMSEC operations and annual IP self-assessments on behalf of the senior host operational commander. Use AF Form 4160.

2.2.2. Provide technical support to visiting IPATs, such as on-line surveys, site traffic, and network mapping information.

2.3. HQ AFCA:

2.3.1. Develops, publishes, and maintains the currency of IP assessment criteria (AF Form 4160).

2.3.2. Periodically accompanies MAJCOMs, and, if requested, assists them during MAJCOM IPAA visits. Keeps visits to the minimum necessary to maintain currency with wing IP and AFNCC functions and responsibilities.

2.3.3. Reviews MAJCOM IPAA summaries and analyses to identify over-all weaknesses in the Air Force IP program and to meet the metrics and assessment requirements of Air Force Policy Directive 33-2, *Information Protection*.

2.3.4. Provides feedback to MAJCOMs.

2.3.5. Tracks and monitors MAJCOMs IPAP schedules.

2.4. Air Force Information Warfare Center. Provides technical support to MAJCOM IPAPs according to AFI 33-207, *Computer Security Assistance Program*.

3. Reports . MAJCOM IPAA reports must reflect the status of the wing IP posture. The reports will include significant problems and deficiencies identified, those resolved on-site, and those that require resolution. The reports will include recommendations and assistance provided by the IPAT.

4. Report Preparation . MAJCOMs document the results of all command IPAAs in a narrative format (see **Attachment 2**). They properly classify IPAA reports and make sure they are marked accordingly and include a rating for the results of the IPAA. This report is exempt from reports control symbol (RCS) reporting according to AFI 33-324, *The Information Collections and Reports Management Program; Controlling Internal, Public, and Interagency Air Force Information Collections*.

5. Information Protection Assessment and Assistance Reports Processing .

5.1. MAJCOM IPAA Reports.

5.1.1. Process reports through channels from the assessed activity's MAJCOM to the appropriate wing IP office. When a command other than the assessed activity's headquarters performs a review, the assessing activity processes the report through its own IP channels to the assessed activity’s IP office. MAJCOM IP offices send information copies of IPAA reports and follow-up reports to HQ AFCA/GCIS.

5.1.2. Assessing authority will process reports within 10 workdays.

5.2. Wing IP Self-Assessments.

5.2.1. Process wing reports through channels to the assessed unit's commander and the assessed office.

5.2.2. Process reports within 10 workdays.

6. Information Protection Assessment and Assistance Report Responses .

6.1. Command and Wing IPAA Report Processing:

6.1.1. Assessed activities must address all deficiencies identified in reports. Replies must address the specific actions needed to correct and eliminate the basic cause of the deficiencies and provide enough detail to permit effective evaluation.

6.1.2. Each reviewing authority must provide a concurrence or nonconcurrence with corrective actions taken and endorse the report to next reviewing authority.

6.1.3. MAJCOM IP offices are the final authority on determining the adequacy of unit responses to command IPAAs and the closing of individual deficiencies or reports.

6.1.4. Wing IP offices are the final authority on determining the adequacy of unit responses to wing IPAAs and the closing of individual deficiencies or reports.

6.1.5. Wing IP activity must provide a copy of the report to the wing commander.

7. Form Prescribed . AF Form 4160, **Information Assurance Assessment and Assistance Program (IAAP) Criteria**.

JOHN L. WOODWARD, JR., Lt General, USAF
Director, Communications and Information

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

AFPD 33-2, *Information Protection*

AFI 33-201, *(FOUO) Communications Security (COMSEC)*

AFI 33-207, *Computer Security Assistance Program*

DELETE AFI 33-208, *Information Protection Operations*

AFI 33-324, *The Information Collections and Reports Management Program; Controlling Internal, Public, and Interagency Air Force Information Collections*

DELETE AFI 37-124, *The Information Collections and Reports Management Program; Controlling Internal, Public, and Interagency Air Force Information Collections* (will convert to AFI 33-324)

DELETE AFSSI 4100, (C) *Communications Security Program (U)*

Abbreviations and Acronyms

AFCA—Air Force Communications Agency

AFCERT—Air Force Computer Emergency Response Team

AFI—Air Force Instruction

AFIWC—Air Force Information Warfare Center

AFPD—Air Force Policy Directive

AFSC—Air Force Specialty Code

ANG—Air National Guard

ASSIST—Automated System Security Incident Support Team

AFNCC—Air Force Network Control Center

COMSEC—Communications Security

CSET—Computer Security Engineering Team

DRU—Direct Reporting Unit

FOA—Field Operating Agency

IAAP—Information Assurance Assessment and Assistance Program

IP—Information Protection

IPAA—Information Protection Assessment and Assistance

IPAP—Information Protection Assessment and Assistance Program

IPAT—Information Protection Assessment and Assistance Team

MAJCOM—Major Commands

RCS—Record Control Symbol

Terms

Computer Security Engineering Team (CSET)—Deployable teams that provide assistance to computer users and Air Force organizations. CSETs also provide assistance to control and recover from intrusion activity.

Information Protection (IP)—Measures to protect friendly information systems by preserving the availability, integrity, and confidentiality of the systems and the information contained within the systems. See AFPD 33-2.

Information Protection Assessment and Assistance Program (IPAP)—A MAJCOM function established to assess the effectiveness of wing IP programs and to provide assistance, when necessary.

Information Protection Operations—Proactive security functions established to assist Air Force organizations to deter, detect, isolate, contain, and recover, from intrusions of computers and computer networks.

Information Protection tools—IP tools perform numerous security functions including boundary protection, viral detection, intrusion detection, configuration inspection, network mapping, remote patching, and on-line surveys determining status of vulnerabilities, etc.

Information Systems—Any telecommunications and/or computer-related equipment or interconnected system or subsystems of equipment that is used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception, of voice, and/or data, and includes computer software, firmware, and hardware. ***NOTE:*** This includes automated information systems.

Suspicious Activity—Suspicious activity includes failed log-ins, changes to privileges, and renamed user account/privileges.

Attachment 2

EXAMPLE REPORT FORMAT FOR RESULTS OF COMMAND INFORMATION PROTECTION ASSESSMENTS AND ASSISTANCE VISITS

MEMORANDUM FOR 0001CG

FROM: MAJCOM IP Office

SUBJECT: Report of Results of Command Information Protection Assessment and Assistance Visit

Section I - General

1. This overall rating of wing COMSEC operations is Satisfactory (AFI 33-230).

2. (Names of IPAA team members) conducted the Command information protection assessment of the 1st Communications Group, Scott AFB IL, Information Protection office from (inclusive dates of the assessment). The assessment provides valuable insight into the information protection posture of (wing/site name). The previous assessment and assistance visit were conducted (date). The authority for this assessment is AFI 33-230.

3. Personnel Contacted:

Colonel Jones, 275AAW Commander

Colonel Parks, 0001CG Commander

Lt Col West, 0001CG Director of Operations

MSgt Young, Wing IP Manager

Section II - Findings/Recommendations

4. Deficiencies Identified Using AF Form 4160.

a. COMSEC.

Item 1.

a. Finding: Ref: AFI 33-XXX, para 4.

b. Recommendation: The XXXXX must ensure:

(1) Thorough self-reviews of the main COMSEC account and each user agency are scheduled and conducted at approximately 6-month intervals.

(2) Use AF Form 4160 to conduct IP assessments.

(3) Document all reviews and forward them through user agency commanders. Aggressively pursue follow-up actions and maintain review reports on file for review during command IPAAs.

b. COMPUSEC.

c. EMSEC.

d. SATE.

Section III - Other Comments:

5. Other Deficiencies.

a.

b.

6. Laudatory Comments.

7. Summary of Assistance Provided.

8. Request you endorse this report through command IP channels within 10 work-days of receipt. If you are unable to correct all deficiencies in the 10 days, then provide the status of the corrective actions underway and include the estimated completion date.

(Signature Block)

Attachment 3

IC 99-1 TO AFI 33-230, INFORMATION PROTECTION ASSESSMENT AND ASSISTANCE PROGRAM

18 JUNE 1999

SUMMARY OF REVISIONS

This change incorporates IC 99-1 (Attachment 3). It requires the MAJCOMs' to send Information Protection Assessment and Assistance Program (IPAP) schedules to HQ AFCA/GCIS and for HQ AFCA to track and monitor the schedules. It tasks gaining MAJCOM's to work with ANG to ensure biennial assessmenst of ANG units are performed.. It changes HQ AFCA/SYSC office symbol to HQ AFCA/GCIS, and HQ USAF/SCTW office symbol to HQ AFCIC/SYIP. It changes "authorities" to "authority" in paragraph 6.1.2. A (|) indicates revision from previous edition.

This instruction establishes the Information Protection Assessment and Assistance Program (IPAP). It applies to the Air Force Information Warfare Center (AFIWC), major commands (MAJCOM), field operating agencies (FOA), direct reporting units (DRU), information warfare squadrons (IWS), Headquarters Air Force Communications Agency (HQ AFCA), and all Air Force information systems users. Send recommended changes or comments to HQ AFCA/XPXP, 203 W Losey St, Rm 1060, Scott AFB IL 62225-5222, using AF Form 847, **Recommendation for Change of Publication**, with an information copy to HQ AFCIC/SYIP, 1250 Air Force Pentagon, Washington DC 20330-1250. See **Attachment 1** for a glossary of references and supporting information.

2.1.1. Implement and manage a command IPAP. Send IPAP schedules to HQ AFCA/GCIS for tracking and monitoring.

2.1.2. Set up IP assessment and assistance (IPAA) teams (IPAT) consisting of personnel with experience in base information infrastructures, information systems, and IP Air Force specialty codes (AFSC).

2.1.3. Conduct biennial assessments of wing IP programs using AFCOMSEC Form 13, **Information Protection Criteria**. If IPATs require technical support from the AFIWC, they must request it at least 60 days prior to scheduled MAJCOM IPAA visits. Gaining MAJCOM's will work with ANG to ensure biennial assessments of ANG units are performed.

2.3.5. Tracks and monitors MAJCOMs' IPAP schedules.

6.1.2. Each reviewing authority must provide a concurrence or nonconcurrence with corrective actions taken and endorse the report to next reviewing authority.

Attachment 4

IC 2000-1 TO AFI 33-230, INFORMATION PROTECTION ASSESSMENT AND ASSISTANCE PROGRAM

28 September 2000

SUMMARY OF REVISIONS

This IC changes the prescribed form from AFCOMSEC Form 13 to AF Form 4160 where referenced. Additionally, this IC corrects some minor administrative items. See the last attachment (Attachment 4) of the publication, IC 2000-1, for the complete IC. A (|) indicates revision from the previous edition.

2.1.3. Conduct biennial assessments of wing IP programs using AF Form 4160, Information Assurance Assessment and Assistance Program (IAAP) Criteria. If IPATs require technical support from the AFIWC, they must request it at least 60 days prior to scheduled MAJCOM IPAA visits. Gaining MAJCOMs will work with ANG to ensure biennial assessments of ANG units are performed.

2.1.4.5. Quality of wing communications security (COMSEC) operations (AFI 33-201, [FOUO] Communications Security [COMSEC]).

2.2.1. Perform semiannual self-assessment of wing COMSEC operations and annual IP self-assessments on behalf of the senior host operational commander. Use AF Form 4160.

2.3.1. Develops, publishes, and maintains the currency of IP assessment criteria (AF Form 4160).

2.4. Air Force Information Warfare Center. Provides technical support to MAJCOM IPAPs according to AFI 33-207, *Computer Security Assistance Program.*

4. Report Preparation. MAJCOMs document the results of all command IPAAs in a narrative format (see Attachment 2). They properly classify IPAA reports and make sure they are marked accordingly and include a rating for the results of the IPAA. This report is exempt from reports control symbol (RCS) reporting according to AFI 33-324, The Information Collections and Reports Management Program; Controlling Internal, Public, and Interagency Air Force Information Collections.

7. Form Prescribed. AF Form 4160, **Information Assurance Assessment and Assistance Program (IAAP) Criteria**.

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

AFPD 33-2, *Information Protection*

AFI 33-201, *(FOUO) Communications Security (COMSEC)*

AFI 33-207, *Computer Security Assistance Program*

DELETE AFI 33-208, *Information Protection Operations*

AFI 33-324, *The Information Collections and Reports Management Program; Controlling Internal, Public, and Interagency Air Force Information Collections*

DELETE AFI 37-124, *The Information Collections and Reports Management Program; Controlling Internal, Public, and Interagency Air Force Information Collections* (will convert to AFI 33-324)

DELETE AFSSI 4100, *(C) Communications Security Program (U)*

Abbreviations and Acronyms

AFCAAir Force Communications Agency

AFCERTAir Force Computer Emergency Response Team

AFIAir Force Instruction

AFIWCAir Force Information Warfare Center

AFPDAir Force Policy Directive

AFSCAir Force Specialty Code

ANGAir National Guard

ASSISTAutomated System Security Incident Support Team

AFNCCAir Force Network Control Center

COMSECCommunications Security

CSETComputer Security Engineering Team

DRUDirect Reporting Unit

FOAField Operating Agency

IAAPInformation Assurance Assessment and Assistance Program

IPInformation Protection

IPAAInformation Protection Assessment and Assistance

IPAPInformation Protection Assessment and Assistance Program

IPATInformation Protection Assessment and Assistance Team

MAJCOMMajor Commands

RCSRecord Control Symbol

Terms

Computer Security Engineering Team (CSET)--Deployable teams that provide assistance to computer users and Air Force organizations. CSETs also provide assistance to control and recover from intrusion activity.

Information Protection (IP)--Measures to protect friendly information systems by preserving the availability, integrity, and confidentiality of the systems and the information contained within the systems. See AFPD 33-2.

Information Protection Assessment and Assistance Program (IPAP)--A MAJCOM function established to assess the effectiveness of wing IP programs and to provide assistance, when necessary.

Information Protection Operations--Proactive security functions established to assist Air Force organizations to deter, detect, isolate, contain, and recover from intrusions of computers and computer networks.

Information Protection Tools--IP tools perform numerous security functions including boundary protection, viral detection, intrusion detection, configuration inspection, network mapping, remote patching, and on-line surveys determining status of vulnerabilities, etc.

Information Systems--Any telecommunications and/or computer-related equipment or interconnected system or subsystems of equipment that is used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception, of voice, and/or data, and includes computer software, firmware, and hardware. ***NOTE:*** This includes automated information systems.

Suspicious Activity--Suspicious activity includes failed log-ins, changes to privileges, and renamed user account/privileges.

Attachment 2

EXAMPLE REPORT FORMAT FOR RESULTS OF COMMAND INFORMATION PROTECTION ASSESSMENTS AND ASSISTANCE VISITS

MEMORANDUM FOR 0001CG

FROM: MAJCOM IP Office

SUBJECT: Report of Results of Command Information Protection Assessment and Assistance Visit

Section I - General

1. This overall rating of wing COMSEC operations is Satisfactory (AFI 33-230).

2. (Names of IPAA team members) conducted the Command information protection assessment of the 1st Communications Group, Scott AFB IL, Information Protection office from (inclusive dates of the assessment). The assessment provides valuable insight into the information protection posture of (wing/site name). The previous assessment and assistance visit was conducted (date). The authority for this assessment is AFI 33-230.

3. Personnel Contacted:

Colonel Jones, 275AAW Commander

Colonel Parks, 0001CG Commander

Lt Col West, 0001CG Director of Operations

MSgt Young, Wing IP Manager

Section II - Findings/Recommendations

4. Deficiencies Identified Using AF Form 4160.

a. COMSEC.

Item 1.

a. Finding: Ref: AFI 33-XXX, para 4.

b. Recommendation: The XXXXX must ensure:

(1) Thorough self-reviews of the main COMSEC account and each user agency are scheduled and conducted at approximately 6-month intervals.

(2) Use AF Form 4160 to conduct IP assessments.

(3) Document all reviews and forward them through user agency commanders. Aggressively pursue follow-up actions and maintain review reports on file for review during command IPAAs.

b. COMPUSEC.

c. EMSEC.

d. SATE.

Section III - Other Comments:

5. Other Deficiencies.

a.

b.

6. Laudatory Comments.

7. Summary of Assistance Provided.

8. Request you endorse this report through command IP channels within 10 work-days of receipt. If you are unable to correct all deficiencies in the 10 days, then provide the status of the corrective actions underway and include the estimated completion date.

(Signature Block)